combine the reference teachings; (2) there must be a reasonable expectation of success; and (3) the combined references must teach or suggest all the claim limitations. MPEP § 2143. A *prima facie* case of obviousness has not been shown.

Nachenberg discloses a dynamic heuristic method for detecting computer viruses that includes a decryption phase, an exploration phase and an evaluation phase (Title and Abstract). Nachenberg purports to be an improvement over prior art virus detection techniques, such as signature scanning, integrity checking and static heuristic detection, and purports to "overcome" various problems encountered in such prior art systems.

The principal advantage alleged by Nachenberg is that previously unknown or undetected viruses can be detected. During the decryption phase, the method emulates a sufficient number of instructions to allow an encrypted virus to decrypt the virus' viral body (Col. 7, lines 3-5). This phase is performed in a fully contained virtual environment that is effectively isolated from actual hardware devices so that no harm can be done by a virus while a file is being simulated (Col. 6, lines 35-39 and 51-58). Ten separate procedures are performed as part of this phase (Col. 7, lines 27-30). During the exploration phase, all sections of code within a region likely to contain any virus are emulated at least once (Col. 7, lines 9-11). The exploration phase includes eight separate procedures (Col. 12, lines 14-16). During the evaluation phase, any suspicious operations observed during the decryption and exploration phases are analyzed to determine whether the target program appears to be infected by a computer virus (Col. 7, lines 17-21). The evaluation phase includes up to six procedures that might be performed depending on whether the behavior of the program is "suspicious." At the end of the entire process, Nachenberg describes one of two possible responses. First, if the suspect program is determined to contain "highly suspicious" combinations, a label corresponding to the combinations detected is returned to the anti-virus main module (Col. 17, lines 50-54). If no "highly suspicious" combination is detected, the anti-virus main module is notified that the file appears to be virus-free (Col. 17, lines 55-58).

Serbinis discloses an Internet-based document management system and method, wherein access to the system and the system's services are controlled through use of access tokens (Abstract). Each access token is a security code comprised of a signed string unique to a transaction and generated from one or more random numbers independent of any user information, resource information or other identifiable information (Col. 5, lines 9-14). Serbinis describes an Internet-accessible server programmed to generate the access tokens and to provide a plurality of document management services (Col. 5, lines 2-6). The document management services include document storage and retrieval, collaborative file sharing, workflow services for electronic documents, an electronic document delivery service, and a document distribution service (Col. 5, lines 4-8).

In contrast, Claim 1 recites a system for distributing portable computer virus definition records with binary file conversion wherein the system comprises a structured virus database, a client database engine and a converter. Claim 1 recites that the structured virus database stores one or more virus definition records, each comprising an identifier uniquely identifying a computer virus, at least one virus name associated with the computer virus, a virus definition sentence comprising object code providing operations to detect the identified computer virus within a computer system and a virus removal sentence comprising object code providing operations to clean the identified computer virus within a computer system. Claim 1 further recites that the client database engine stores at least one updated virus definition record into the structured virus database indexed by the identifier and the at least one virus name for each virus definition record. Claim 1 further recites that the converter converts the virus definition records stored in the structured virus database into a virus data file comprising virus definition sets, each virus definition set comprising binary data encoding instructions to detect the computer virus within a computer system, instructions to clean the computer virus from the computer system and names associated with the computer virus.

In contrast, Claim 10 recites a method for distributing portable computer virus definition records with binary file conversion comprising the steps of storing one or more virus definition records into a structured virus database, storing at least one updated virus definition record into the structured virus database and converting the virus definition records stored in the structured virus database into a virus data file comprising virus definition sets. Claim 10 further recites that each virus definition record comprises an identifier uniquely identifying a computer virus, at least one virus name associated with the computer virus, a virus definition sentence comprising object code providing operations to detect the identified computer virus within a computer system, and a virus removal sentence comprising object code providing operations to clean the identified computer virus from the computer system. Claim 10 further recites that the updated virus definition record is indexed by the identifier and the at least one virus name for each virus definition record. Claim 10 further recites that each virus definition set comprises binary data encoding instructions to detect the computer virus within a computer system, instructions to clean the computer virus from the computer system and names associated with the computer virus.

In contrast, Claim 20 recites a method for updating a binary computer virus data file from virus definition records stored in a structured virus database, comprising means for storing virus definition records into a structured virus database, each virus definition record comprising an identifier, at least one virus name, a virus definition sentence defining operations to detect the identified computer virus, and a virus removal sentence defining operations to clean off the identified computer virus. Claim 20 further recites means for comparing subsequently modified versions of the structured virus database to form a delta set of virus definition records and means for storing the delta virus definition records set into the structured virus database. Claim 20 further recites means for converting the virus definition records stored in the structured virus database into a virus data file comprising virus definition sets, each virus definition set comprising binary instructions to detect the computer virus, binary instructions to clean off the computer virus, and names associated with the computer virus.

First, Nachenberg fails to provide a suggestion or motivation to combine with the reference teachings of Serbinis. Nachenberg teaches a method for detecting computer viruses using a dynamic heuristic approach to detecting viruses. Nachenberg allegedly distinguishes over signature scanning anti-virus programs that work by scanning files for signatures of known viruses. Rather, the approach taught by Nachenberg has the capability of detecting previously unknown or undiscovered viruses and relies on emulating the operation of suspect programs to determine if the program appears virus-like. Furthermore, Nachenberg simply detects viruses. Upon completing an evaluation of a suspect program, Nachenberg returns a message that the suspect program appears virus-free or appears to contain a virus. Nachenberg is silent as to what, if any, action is taken following notification. Nothing in Nachenberg suggests any need for, or desirability of combining with, a document management system.

In particular, Nachenberg makes reference to prior art signature scanning antivirus programs, but such reference similarly fails to provide a suggestion or motivation to combine with Serbinis. Nachenberg teaches only a dynamic heuristic approach to detecting computer viruses and is silent as to what happens once a virus is detected following notification. Again, the teachings of Nachenberg, and, in particular, Nachenberg's discussion of prior art signature scanning virus detection techniques, fail to provide a suggestion or motivation to combine with the Internet-based document management system taught by Serbinis.

Serbinis also fails to provide a suggestion or motivation to modify or combine with the teachings of Nachenberg. Serbinis teaches storing documents without teaching that such documents themselves concern virus data. Serbinis does state that documents can optionally be scanned for viruses, if desired, before being stored (Col. 10, lines 47-48). However, documents that might contain viruses are not the same as documents containing information about viruses, the latter of which is neither taught nor suggested by Serbinis. Thus, Serbinis' reference to scanning documents for viruses does not teach that storing documents is a necessary or desirable part of detecting viruses. Nor does Serbinis teach or

suggest the storing of virus data. As a result, one of ordinary skill in the art would not perceive any reason to combine the Internet-based document management system of Serbinis with the dynamic heuristic virus detection method of Nachenberg.

Second, one of ordinary skill in the art would not have a reasonable expectation of success in combining the teachings of Nachenberg and Serbinis. Nachenberg teaches a dynamic heuristic approach whose chief advantage is detecting new or previously-undiscovered viruses. Serbinis, which is concerned with providing access tokens in an Internet-based document management system, discloses no form of virus protection. If Nachenberg were to be combined with Serbinis, the result would be a dynamic heuristic virus detection method, wherein records containing only virus identification information would be available over the Internet to selected users possessing appropriate access tokens. Given that Nachenberg fails to teach or suggest maintaining virus information records, why or how such combination would be desirable or useful is speculative.

Finally, even if combined, the Nachenberg and Serbinis references fail to teach or suggest all claim limitations. Nachenberg fails to teach or suggest what action is taken once a virus is detected. Nachenberg is concerned only with detecting new or previously-undiscovered viruses. Accordingly, Nachenberg does not disclose such claim elements as a virus removal sentence comprising object code providing operations to clean the identified computer virus within a computer system, per Claims 1, 10 and 20. Although Nachenberg indicates that "a signature scanning antivirus program can identify particular virus strains for removal," Nachenberg fails to teach or suggest how the actual virus removal should be accomplished. Again, Nachenberg is concerned only with detecting viruses, not taking action beyond notification once a virus is detected. Nachenberg also fails to teach or suggest (1) an identifier uniquely identifying a computer virus, (2) at least one virus name associated with the computer virus, and (3) a virus definition sentence comprising object code providing operations to detect the identified computer virus within the computer system, per Claims 1, 10 and 20. Rather, Nachenberg teaches that (1) signature scanning antivirus

programs exist, (2) that such programs utilize "signatures" that are extracted and stored in a database, (3) that such programs scan a target program "to detect the presence of a virus signature," and (4) that "if a signature is found . . . the target program is deemed infected" (Col. 1, lines 27- 45).

In addition, Serbinis fails to teach or suggest converting virus definition records into a virus data file comprising virus definition sets, per Claims 1, 10 and 20. Serbinis teaches that, if desired, documents can be scanned for viruses before being stored, but fails to teach or suggest a virus definition set and, in particular, any form of document or record including (1) binary data encoding instructions to detect a computer virus within a computer system, (2) instructions to clean the computer virus from the computer system, and (3) names associated with the computer virus. The binary data encoding instructions recited by claims 1, 10 and 20 further include computer executable code operable to detect a computer virus within a system. Serbinis, however, fails to teach or suggest such structure and also fails to teach or suggest binary data encoding instructions. Accordingly, all claim limitations are not found in Nachenberg and Serbinis.

In view of the foregoing, (1) no suggestion or motivation exists to combine the teachings of Nachenberg with those of Serbinis, (2) there is no expectation of success if the teachings are combined, and (3) the combined references fail to teach or suggest all the claim limitations. Thus, a *prima facie* case of obviousness has not been shown with respect to Claims 1, 10 and 20.

Claims 2-9 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 11-19 are dependent on Claim 10 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. As a *prima facie* case of obviousness has not been shown, withdrawal of the rejection of Claims 1-20 for obviousness under 35 U.S.C. 103(a) is requested.

The prior art made of record and not relied upon has been reviewed by the applicant and is considered to be no more pertinent than the prior art references already applied.